情報処理安全確保支援士試験　本試験分析と傾向と対策法

午後試験が1本化されました

■情報処理安全確保支援士試験の位置づけ

情報処理安全確保支援士は次の役割を担います。

業務と役割

情報セキュリティマネジメントに関する業務，情報システムの企画・設計・開発・運用におけるセキュリティ確保に関する業務，情報及び情報システムの利用におけるセキュリティ対策の適用に関する業務，情報セキュリティインシデント管理に関する業務に従事し，次の役割を主導的に果たすとともに，下位者を指導する。

1　情報セキュリティ方針及び情報セキュリティ諸規程（事業継続計画に関する規 程を含む組織内諸規程）の策定，情報セキュリティリスクアセスメント及びリスク対応などを推進又は支援する。

2　システム調達（製品・サービスのセキュアな導入を含む），システム開発（セキュリティ機能の実装を含む）を，セキュリティの観点から推進又は支援する。

3　暗号利用，マルウェア対策，脆弱性への対応など，情報及び情報システムの利用におけるセキュリティ対策の適用を推進又は支援する。

4　情報セキュリティインシデントの管理体制の構築，情報セキュリティインシデ ントへの対応などを推進又は支援する。

(IPA試験要綱Ver5.3より抜粋)

■午前試験

★午前Ⅰ試験

午前Ⅰ（高度共通区分）試験は，4肢択一式で30題出題されます。試験時間は，50分間（9:30～10:20）です。また，合格基準は，正答数60％（18題正解）です。午前Ⅰ試験で合格基準に達さないと，いわゆる「足きり」となってしまい，残りの試験（午前Ⅱ，午後）は採点されません。一方，試験全体としての合否と関係なく，午前Ⅰ試験で合格基準に達していると，次回以降（2年間）の午前Ⅰ試験が免除されます。なお，応用情報技術者試験，高度区分の情報処理技術者試験に合格していても，合格時から2年間，午前Ⅰ試験が免除されます。

試験問題は，同日に実施される応用情報技術者試験の午前問題から30題抜粋して作成されています。近年は，

テクノロジ系問題…17題，マネジメント系問題… 5題，ストラテジ系問題… 8題

での出題です。今後ともに，この傾向は続くものと考えられます。テクノロジ系問題が若干多いですが，マネジメント・ストラテジ系問題も4割以上を占めます。したがって，**両分野ともにしっかりと学習して対策をしておく必要があります**。レベルは，応用情報技術者試験からの抜粋であることから明らかなように，応用情報技術者試験と同一レベルです。**応用情報技術者試験の受験経験の無い方は，午前Ⅰ試験対策に，ある程度(かなり)の時間を要します。この分の学習時間をしっかり確保してください**。

★午前Ⅱ試験

午前Ⅱ試験は，4肢択一式で25題出題されます。試験時間は，40分間（10:50～11:30）です。また，合格基準は，正答数60％（15題正解）です。午前Ⅱ試験で合格基準に達さないと，いわゆる「足きり」となってしまい，残りの試験（午後）は採点されません。試験時間も短く慌ただしい試験になります。ゆっくり解いているとすぐに時間が経ってしまいますので注意しましょう。

R06年春試験では，

・セキュリティ分野	…	17題 (問1～17)	《レベル4》
・ネットワーク分野	…	3題 (問18～20)	《レベル4》
・データベース分野	…	1題 (問21)	《レベル3》
・システム/ソフトウェア開発分野	…	2題 (問22，23)	《レベル3》
・サービスマネジメント分野	…	1題 (問24)	《レベル3》
・システム監査分野	…	1題 (問25)	《レベル3》

での出題でした。例年と比べて分野ごとの出題数に変化はありません。

セキュリティ分野は，CSRF対策，MAC，SAML，DoS，CRL，FIPS PUB140-3，HSTSなど，**テキストで学習して知っているべき基本用語（知識）が主として出題**されていました。テキストに掲載の用語を定着させ，過去問演習をしっかりしていれば，合格点は得点できるレベルの試験です。再出題の問題が約6割でした。

新出用語は，次回以降，午後試験のテーマとして取り上げられる可能性も視野に入れて，Webや専門書などで，詳しく学習しておくと良いです。

午前Ⅰ試験が免除の方は，システム/ソフトウェア開発，サービスマネジメント，監査分野について，一通りの知識整理をしておくとよいです。セキュリティとネットワークに自信があれば，この2分野だけでも合格ラインには達せますから，おおざっぱに知識の確認を行う程度ですませておくのも策でしょう。

■午後試験

午後試験は，事例問題，記述式の試験です。４問出題され，2問を選択して解答します。試験時間は150分，合格点は60点です。前回は，問題によって，分量にばらつきがありましたが，今回は，4問とも従来の午後II試験問題に近い分量に増えていました。従来の午後II試験問題ほど込み入った事例ではありませんでしたが，読む分量が多い（1問当たり10ページ程度）ですから，長文読解が苦手な人には解きづらかったです。

午後試験問題の特徴として，テーマで取り上げている話題に関する知識があるかないかで解きやすさが全く違うという点が挙げられます。標的型攻撃（電子メールによる攻撃），Webアプリケーションを狙った攻撃，スマートホンに関するセキュリティ，組込み機器のセキュリティ，クラウドサービスでの認証連携，インシデント対応などのテーマが好んで出題されます。近年は，特に，認証に関する問題が頻出です。解答は教科書的なものが多いので，なるべく最新のセキュリティテーマに触れ，どのように対策するのが一般的なのかといった知識を増やしてください。

今回は，全て技術系の問題で，なおかつ，3問（問1，問2，問4）がWeb技術に関する問題でした。HTTPについてしっかり知っていることが求められます。セキュリティ技術に詳しくないと合格は難しいと言えます。さらに，字数制限がない問題が全ての問にありました。このような問題は，知識が定着していないと一言しか書けず，その結果，正解となりません。午後試験は，ますます，丸暗記や山を掛けた学習が通用しない試験になったと言えます。

今回も認証認可を扱った問題が3問出題されています。セキュリティの大きなテーマの一つですから，重点学習テーマといえます。

問1　APIセキュリティ
問2　サイバー攻撃への対策
問3　Webセキュリティ
問4　Webアプリケーションプログラム（セキュアプログラミングJava）

です。セキュアプログラミングに関する問題は前回も出題されていますから，定番になりそうな雰囲気を感じます。（一方で，H31～R4まで，4年間出題されなかった時期もあったことを忘れてはいけません。作問者がネタ切れになれば，当然出題されないでしょう）

問1は，**認証，認可**，WAFのルール設定に関する問題です。認証とは何かという基本が理解できていれば，何を問われているのか判断できます。HTTPについてもよく知っている必要があります。50点満点を得点することは難しいと考えますが，合格点の60%（30点）は，得点できる問題です。

問2は，リモートワーク用のVPN装置への攻撃やDDoS攻撃に関する問題です。事例を丁寧に読めば答えられる問題が多かったです。**認証**，DNSのセキュリティ，ネットワークセキュリティが題材です。

問3は，Webアプリケーションの脆弱性に関する問題です。プログラム言語の知識は不要ですが，HTTPについての知識が十分に備わっていないと解答できません。XSS，CSRF，SSRF，**認可制御**の不備が題材です。

問4は，Java言語を用いたセキュアプログラミングの問題です。LinuxなどのUnix系OSを利用した経験も必要であったと考えます。chmodコマンドで，770は何を意味しているのかわからなければ解けませんでした。空欄hは，Java言語の文法に関する問題で，過去の基本情報技術者試験のJavaプログラミングの問題にも登場するようなものでした。セキュアプログラミングの問題は，いまからプログラム言語を習得するという方には不向きなテーマです。このテーマを選択するには，現時点で，過去の基本情報技術者試験のC言語，Java言語の問題で，60%以上は正解できるプログラミング力が必要です。

■学習にあたって

・午前試験は過去問演習で攻略可能です。出来る限りたくさん演習しましょう

・午後試験は，問題文を正確に読んで，状況を的確に把握することが最も重要です。また，試験要綱の記載の**支援士の役割**を念頭に，解答の方向を察する練習してください。

・情報セキュリティマネジメントの視点でも知識整理をしておきましょう。

・Webアプリケーションのセキュリティ，DNSサーバのセキュリティ，メールサーバのセキュリティ，標的型攻撃，認証認可技術（SAML，OAuth，Keycloakも注目かもしれません）は，重点的に学習してください。さらに，HTTP自体の知識もしっかり習得してください。

・ログ調査，ログ分析などができるように，日頃から各サーバのログを見ておくとよいです。

・仮想サーバの運用についても知識を持っておきましょう。特に，コンテナ型の仮想化は近年多く使われています。詳しく学習しておくとよいです。

・ネットワークセキュリティ（VLAN，無線LAN，TLS1.3，VPNなど）も学習を忘れずに！

・IPAのセキュリティサイト(http://www.ipa.go.jp/security)は必見です！

・セキュリティに関する情報を日頃から幅広く集めることは，この職種にかかわる者として必須です。実践しましょう。

・過去問題演習は，PM I (1.5時間のまとまった時間が必要) → PM I → PM II (2.5時間のまとまった時間が必要) の繰り返しで演習するとよいです。 AM II は，すきま時間を利用して演習しましょう。